Title: CSD Printer Firmware Compromise - Evidence Archive
Date: 2025-05-31
Analyst: fighting-for-freedom

Overview:

This archive contains forensic data from a hostile binary named `csd-printer` found on an ASUS TUF Gaming A16 laptop running Linux. The binary was **not user-installed** and was **executing silently during boot**. It shows evidence of:

- Unauthorized systemd hooks
- Infinite event polling (`poll()`, `futex()`, `read()` etc.)
- Suspicious interprocess socket writes
- No valid service registration
- No corresponding package or legitimate origin
- Denial or dismissal by authorities despite technical proof

Contents:

- `csd-printer` ELF binary
- `csd-printer-full.trace`: Full syscall trace from `strace`
- `csd-trace.log.*`: Per-thread syscall logs
- `csd-printer-full.tar.gz`: Combined trace archive
- `csd-hashes.md5`, `csd-hashes.sha1`, `csd-evidence-bundle.sha256`: Hash verification files
- `csd-printer-metadata.json`: Metadata for archive.org
- This `README.txt`

SHA256 (csd-printer):
69e0197d8672e4b65a5f13581c4ada4659d236a8894ff3eb40167acf6a467122

Use Cases:

- Threat intelligence sharing
- Upload to VirusTotal and Hybrid Analysis
- Digital forensic validation
- Law enforcement evidence chain
- Civil rights protection documentation

License:

Public Domain / CC0 — Share freely and widely.

Signed with honor and integrity,
- fighting-for-freedom